020112 Controlling Remote User Access

Purpose: To require users of State information technology systems who access agency information technology systems remotely to do so in a secure manner.

STANDARD

Authorized users of agency computer systems, the State Network and data repositories shall be permitted to remotely connect to those systems, networks and data repositories for the conduct of State-related business only through secure, authenticated and carefully managed access methods.

Access to the State Network and agency internal networks via external connections from local or remote locations including homes, hotel rooms, wireless devices and off-site offices shall not be automatically granted with network or system access. Systems shall be available for on- or off-site remote access only after an explicit request is made by the user and approved by the manager for the system in question.

Opening uncontrolled or unsecured paths into any element of the State Network that requires security or to internal computer systems presents unacceptable risk to the entire State infrastructure.

Statewide Standard for Remote Access

Access shall be permitted through an agency-managed secure tunnel such as a Virtual Private Network (VPN) or other open standard protocol such as Secure Shell (SSH) or Internet Protocol Security (IPSec) that provides encryption and secure authentication.

Authentication

- The authentication and authorization system for remote access shall be managed by the agency. Agencies that need centralized network infrastructure services, such as Public Key Infrastructure (PKI), shall use the state-wide authentication and authorization service known as NCID .
- Authentication for remote access shall be strong. Passwords shall not traverse the network in clear text and must meet minimum requirements as documented in approved security policies and standards. Each user who remotely accesses an internal network or system shall be uniquely identifiable.

Users

- User IDs: All users who require remote access privileges shall be responsible for the activity performed with their user IDs. User IDs shall never be shared with those not authorized to use the ID. User IDs shall not be utilized by anyone but the individuals to whom they have been issued. Similarly, users shall be forbidden to perform any activity with user IDs belonging to others.
- Revocation/modification: Remote access shall be revoked at any time for reasons including non-compliance with security policies, request by the user's supervisor or negative impact on overall network performance attributable to remote connections. Remote access privileges shall be

terminated upon an employee’s or contractor’s termination from service. Remote access privileges shall be reviewed upon an employee’s or contractor’s change of assignments and in conjunction with regularly scheduled security assessments.

- Anonymous interaction: With the exception of Web servers or other systems where all regular users are anonymous, users are prohibited from remotely logging into any ITS system or network anonymously (for example, by using “guest” user IDs). If users employ system facilities that allow them to change the active user ID to gain certain privileges, they must have initially logged in employing a user ID that clearly indicates their identity.

Configuration

- Default to denial: If an agency computer or network access control system is not functioning properly, it shall default to denial of access privileges to users. If access control systems are malfunctioning, the systems they support must remain unavailable until such time as the problem has been rectified.
- Privilege access controls: All computers permanently or intermittently connected to external networks must operate with privilege access controls approved by the agency. Multi-user systems must employ user IDs unique to each user, as well as user privilege restriction mechanisms, including directory and file access permissions.
- Antivirus and firewall protection: External computers or networks making remote connection to internal agency computers or networks shall utilize an agency-approved active virus scanning and repair program and an agency-approved personal firewall system (hardware or software). The agency shall ensure that updates to virus scanning software and firewall systems are available to users. External computers or networks making a remote connection to a public Web server are exempted.
- Time-out:
    - Network-connected single-user systems, such as laptops and PCs, shall employ agency-approved hardware or software mechanisms that control system booting and that include a time-out-after-no-activity (for example, a screen saver). To the extent possible, all systems accepting remote connections from public-network-connected users (users connected through dial-up phone modems, dial-up Internet service providers, or broadband, i.e., DSL or cable modems) shall include a time-out system. This time-out system must terminate all sessions that have had no activity for a period of thirty (30) minutes or less. An absolute time-out shall occur after twenty-four (24) hours of continuous connection and shall require reconnection and authentication to re-enter the State Network. In addition, all user IDs registered to networks or computers with external access facilities shall be automatically suspended after a period of thirty (30) days of inactivity.
    - Agencies shall conduct a risk assessment and determine the appropriate time-out period, if any, for hand held devices, (e.g. smart phones, personal data assistants, and Blackberry like devices), that connect to the State Network. The risk assessment shall balance the business needs for immediate access to the hand held device against the security risks associated with the loss of the device. Agencies shall also comply with any legal and regulatory

requirements associated with the information that may contained on the device, such as requirements for confidentiality, security and record retention.[1]

- Failure to authenticate: To the extent possible, all systems accepting remote connections from public-network-connected users shall temporarily terminate the connection or time out the user ID following a sequence of several unsuccessful attempts to log in. For example, if an incorrect dynamic password is provided three consecutive times, dial-up systems shall drop the connection. Repeated unsuccessful attempts to remotely establish a connection using a privileged user ID shall not result in the revocation (suspension as opposed to time-out) of the user ID because this could interfere with the ability of authorized parties to respond to security incidents.

- Modems on desktop/laptop systems: Management must approve the use of modems and the communications software used with modems. Existing modems connected to a LAN that are used for remote control and file transfer from a remote location to LAN desktops must be replaced as soon as possible with a secure TCP/IP or VPN connection. Unless a dynamic password system is installed, workers with home-based, mobile or telecommuting PCs shall not leave modems in auto-answer mode, with communications software enabled, such that incoming dial-up calls could be received.

- VPN and/or other secure communication protocols shall be used to communicate with agency business systems.

- For client-to-server/gateway VPN solutions, split tunnelling shall not be permitted (via configuration option).

Access to Single-Host Systems

- Remote access to single-equipment hosts (i.e., agency servers, Web-hosting equipment) shall be permitted provided that these requirements are met:

    - □ Dial-up modem service: An agency shall provide dial-up modem service *only if* that service is limited exclusively to agency employees and contractors.

    - □ Web-hosting servers shall provide anonymous or authenticated access to pages *only if* the service host prevents onward connection to the State Network.

- Management consoles and other special needs: Users requiring modem access for “out of band” management or special needs must obtain agency security administrator approval for the modem and its use as set forth in agency procedures. Each agency shall establish procedures to approve modems on an individual basis. Any dialup server that grants network access must authenticate each user, minimally, by a unique identification with password and shall encrypt the data stream. All calls must be logged, and logs of access shall be retained for ninety (90) days. At the completion of each dial-up session to a server, the accessing workstation shall be secured via password.

[1] *See,* **120201** Managing Media Storage and Record Retention

Miscellaneous

- Disclosure of systems information: The internal addresses, configurations and related system design information for agency computers and networks shall be kept confidential and shall not be released to third parties who do not have a demonstrable need to know such information. Likewise, the security measures employed to protect agency computers and networks shall be kept confidential and shall be similarly protected.
- Systems shall support the capability for all remote access occurrences to be logged (user ID, date/time, and duration of connection at a minimum).
- There shall be certain remote-access users who warrant use of file/disk encryption technology. This is based on whether confidential records are included in the information that they are able to store on their local systems.
- Audit: Audit logs of remote-access activities shall be maintained for at least ninety (90) days.

Related information

Standard 050404	Working from Home or Other Off-Site Location

ISO 27002 REFERENCE

11.4.2 User authentication for external connections